AD-A103 200 NAVAL UNDERWATER SYSTEMS CENTER NEWPORT RI F/G 9/2
ADP SECURITY AND PRIVACY.(U)
AUG 79 P A ELLIS
UNCLASSIFIED NUSC-TD-5750 NL

END
DATE FILMED
9 81
DTIC

ADP SECURITY AND PRIVACY: BE AWARE

Introduction

Lack of security and privacy are two very common problems facing those involved with computers today. Many people in the computer business are simply not aware of or are apathetic to ADP (automated data processing) security and privacy matters.

Loss of security and privacy is, however, a very real threat in today's highly automated world. Without strict security and privacy regulations, data could be lost, stolen, or manipulated. Since much modern data are beginning to be stored in ADP systems, misuse, mismanagement, or just plain carelessness could result in major problems for a great number of people.

Some security can be built into ADP hardware and software during the developmental phase, but, at the present time, no system is completely secure. It is the responsibility of computer users/custodians to maintain a high level of security and privacy for all computer files.

Because of the obvious lack of awareness concerning security and privacy, the following questions need to be answered:

1. What do the terms "security" and "privacy" mean when used in connection with ADP hardware and software?
2. What happens when there is a lack of security? of privacy?
3. What are some of the causes of this lack of security and privacy?
4. Who has the ultimate responsibility for maintaining security and determining privacy requirements?
5. What are some of the possible solutions for these problems?

Security—What Is It?

According to Webster, security is a state of being or feeling secure: freedom from fear, anxiety, danger, doubt, etc. It is also a state or sense of safety or certainty.

How Does Security Relate to ADP Systems?

In order to have a secure ADP system, only those with a "need-to-know" should have access to data. Security also means that data in ADP systems should be correct and their integrity intact. In other words, security refers to the protection of resources from damage and the protection of data against accidental or intentional disclosure or unauthorized modification or destruction.

What Are ADP Systems?

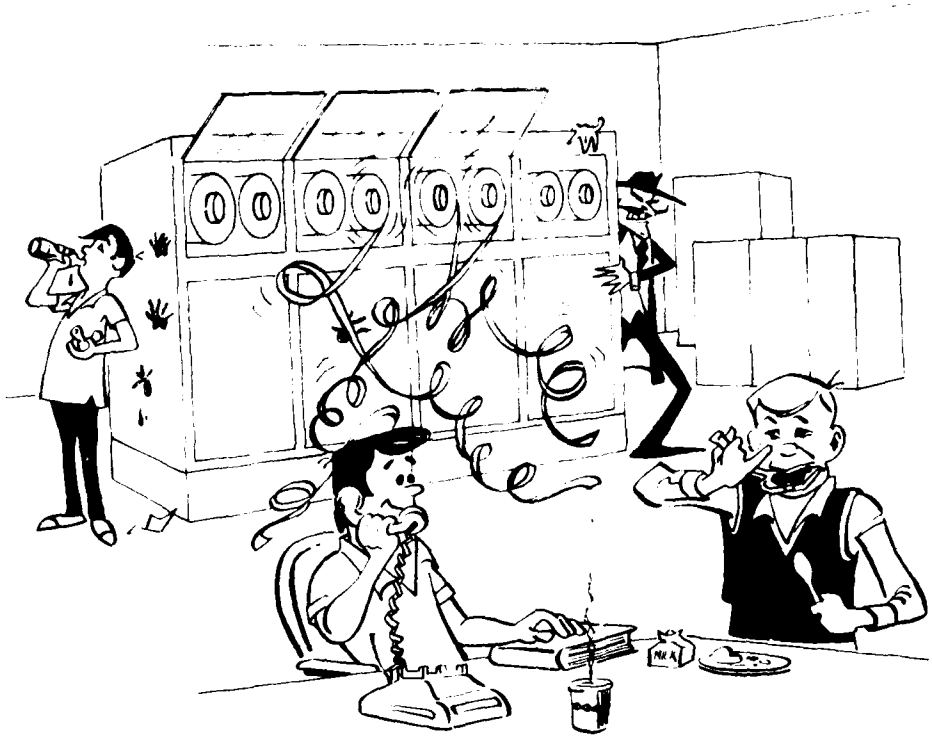
Automated data processing systems are *primarily, but not solely, computers.* An ADP system is essentially made up of six elements:

1. its physical environment
2. People dealing with the system
3. Communications
4. Policies and procedures
5. Hardware, and
6. Software

Why Is Security Such a Problem?

Security in ADP systems is becoming a problem in direct proportion to the increase in the number of computer systems becoming available. One major reason computers face security problems is because they are located in a hostile environment. Such vulnerability stems from the following factors:

1. Complexity
2. Speed of operation
3. Vast amounts of data
4. Inadequate audit trails
5. Telecommunications
6. Complicated operating systems, and
7. Lack of understanding about security aspects.



"I can talk all day if I want to; that computer all but runs itself. Anyway, the other guys are keeping an eye on it."

The security aspects of ADP systems can be defined as:

1. Large scale data bases containing sensitive information,
2. Remote access considerations,
3. Constant growth in numbers of users, and
4. Increase in numbers of personnel with technical knowledge required to access computer systems.

Why Are Security Problems on the Rise?

In today's complex world, there is an increased dependency upon computer systems for critical and sensitive applications. Dependency also stems from a lack of manual back-up systems and inadequate contingency planning.

Although there is an increased dependency upon computers, there has been apathy or a lack of awareness concerning security because of work exigencies. There is also the matter of limited resources that require careful consideration of priorities.

In other words, because of the great demand for fast, efficient computer services, security has not been completely and competently maintained.

Are There Any Other Security Problems?

In addition to the vulnerabilities produced as a by-product of the computer industry growth, there are certain very real threats to security including:

1. Natural hazards
   - Fire,
   - Flood,
   - Severe storm,
   - Failure of electrical power (e.g., air conditioning),
   - Communications failure, and
   - System failure.

2. Accidental errors, omissions, or failures
   - User errors,
   - Operator errors,
   - Data preparation errors,
   - Application program errors,
   - Output errors,
   - System errors,
   - Communication errors, and
   - Inadvertent release of sensitive information.

3. Deliberate acts of computer abuse
   - Fraud
   - Embezzlement
   - Theft
   - Malicious damage
   - Unauthorized use of facilities
   - Sabotage
   - Espionage, and
   - Contractor abuse.

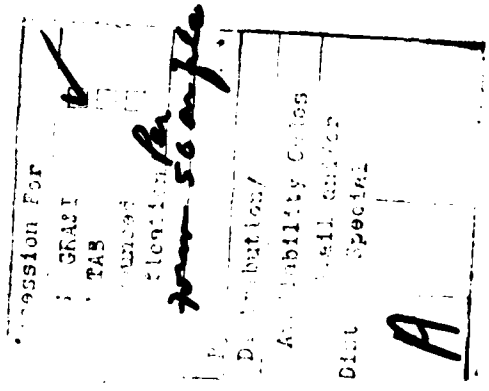
What Can Be Done About Such Threats?

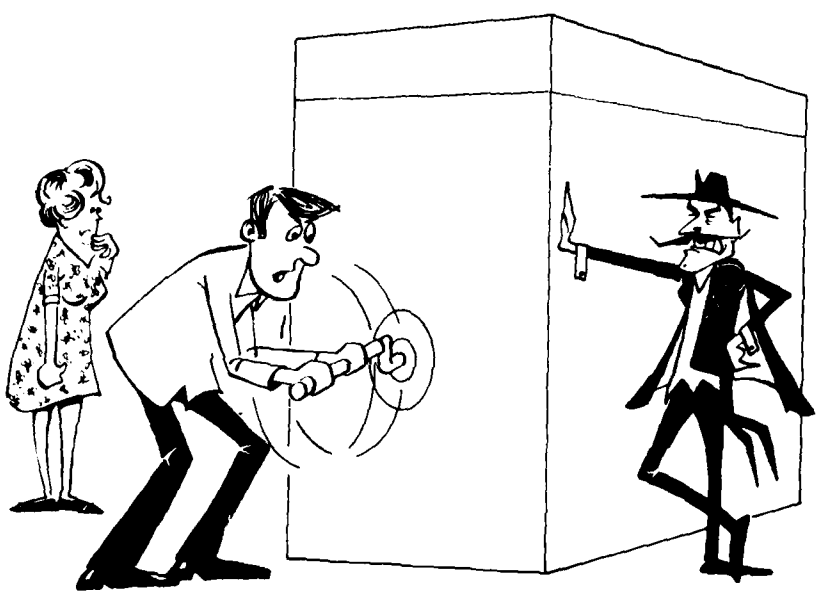
It would be difficult, if not impossible, to prevent natural hazards. However, accidental errors, omissions, or failures, and deliberate computer abuses are problems that can be kept to a minimum with proper maintenance and surveillance. Although security should be built into a system, no system can be really secure unless the user makes it secure. To put this another way, no matter how many security "gadgets" are used, a secure system is *no better* than the person using it. Security must be a personal matter with every computer operator and user in order to have a significant impact.

Who Is Actually Responsible for Security?

It is the *responsibility* of the system designers and manufacturers to build security into an ADP system. Users have the responsibility to maintain a careful watch on their security practices. Management is also responsible since they should set up security requirements and regulations for their employees. In addition, the vendors and users should work together to *determine who is responsible* for what computer security function.

It should be kept in mind, though, that when a security system is being set up, requirements and regulations should be easily understood and workable. *Too much restriction and too much* regulation are as bad as too little of either one.





Those damned oil companies! This is the third blackout this week!"

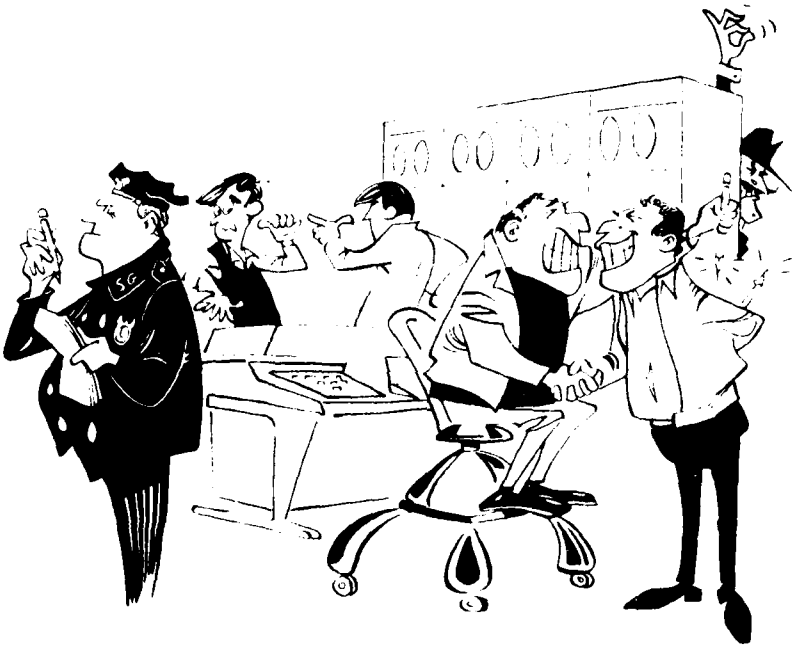
What Roles Do Management and Users Play in Security Problems?

In most cases, management plays a key role in the problems associated with security. In general, most managers are mission-oriented. They are more concerned with the ultimate product than with the production process. Management has recently become more aware of the critical problems associated with computer security and they are taking strong measures to resolve those problems.

Individual users also have problems with security. There seems to be a lack of concern with regard to system security. The user has a tendency to view a computer as just another inanimate object, and yet, this inanimate object still presents a challenge to him. In most cases, a user will not consider computer abuse (on a small scale) a crime. Computer system users can also be lax about reporting known security violations because they don't realize that it can jeopardize their own security.

There is also another problem regarding user security. Many computer users feel that the classification of data is the responsibility of those involved with computer operation rather than that of computer users. In fact, classification rests in the hands of subject matter specialists, not computer operations people.

Today's computer world is marked by rapid growth and extension of applications, continued growth in the numbers of systems (especially mini- and micro-computers), and large increases in the numbers of people involved in data processing. In such an environment, management's lack of involvement and users' apathy serve only to compound the ADP security problem.



"Now, let's see. The programmer said it was the operator's fault; the operator blames his supervisor; the supervisor says that his secretary did it; and the . . . ."

Privacy—What Is It?

Webster defines privacy as the quality or condition of being private; withdrawal from public view or company; seclusion; secrecy. It can also be one's private or personal affairs.

How Does Privacy Relate to ADP Systems?

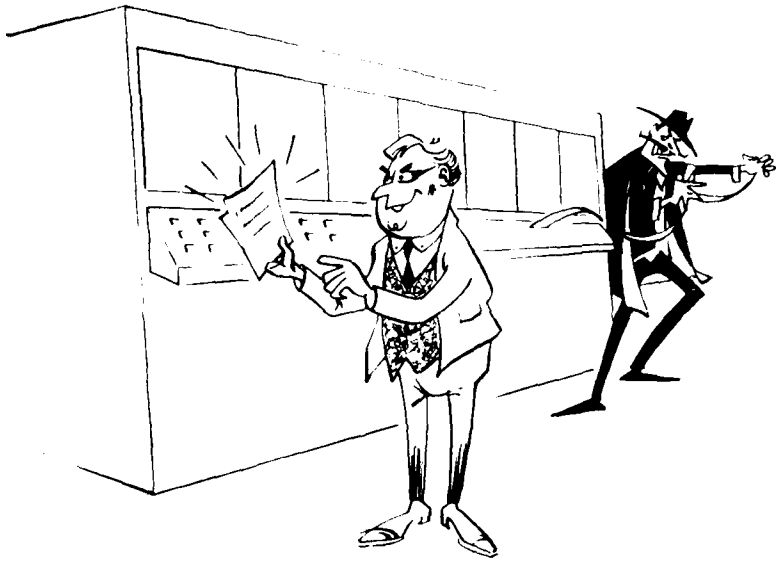
First of all, one must realize the amount of sensitive personal data that is stored in today's computers. A person's entire history is recorded including financial data, medical records, military files, and so forth. An ADP system becomes a storehouse of valuable, but in many cases, very private information. Privacy then, refers to the rights of individuals and organizations to determine for themselves when, how, and to what extent information about them is to be transmitted to others. Privacy is an issue that goes far beyond computer centers and can be thought of as a "people problem" since people, not machines, affect it.

Who Could Gain from Use of Personal Data?

A person who gained access to data files without a "need-to-know" could cause many problems, not only for the private citizen but for others as well. He or she could, for example:

1. Manipulate data.
2. Modify falsify data.
3. Acquire proprietary information and programs.
4. Alter stored programs.
5. Change master files.
6. Access passwords algorithms, or
7. Deny authorized access.

In other words, someone could deliberately abuse computer files to affect many aspects of a person's life such as his credit rating, employment records, even his community standing.



"Just as I suspected; he was fired from his last job."

Has Anything Been Done to Prevent Such Acts?

Congress passed the "Privacy Act of 1974" which sets up certain guidelines regarding privacy and data stored in computers and manual files. In essence, Congress recognized that a person does have a right to privacy, including privacy with regard to personal files. However, there are instances when such files would be made available to authorized persons upon request.

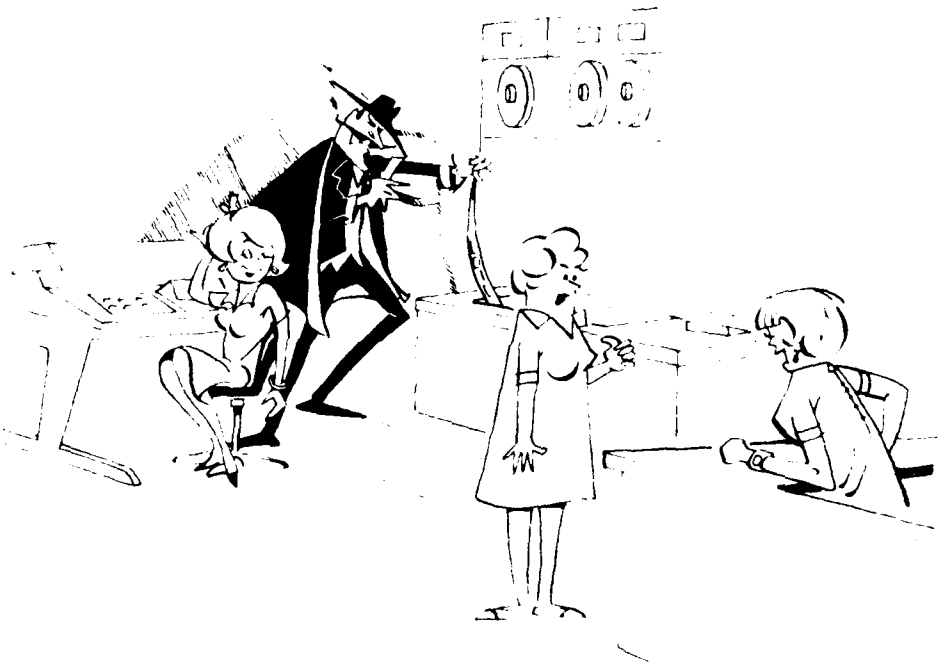
What Are the Custodian's Responsibilities Concerning Privacy?

The custodian has a responsibility to determine information necessary when a request has been received for file information. The accuracy standards should also be determined, along with identification of protection requirements, and the establishment of the sensitivity of requested information.

The custodian should also determine how the use of the information requested could adversely affect the particular individual involved. He can do this by considering the following criteria:

1. What is adverse?
2. What data are vital?
3. What should be done if vital information is in error?
4. What should be done if vital information is disputed?
5. What should be done if vital information is missing?
6. How much impact will an error correction have on a system?

A determination should also be made as to the "need-to-know."



"You know that handsome technical writer in Bldg. 104? He's a GS-15, he's divorced, and he's only 35 years old!"

Summary of ADP Security/Privacy Problems

The typical problem areas with regard to computer security are as follows:

1. Insufficient emphasis on computer security (i.e., inadequate security planning/contingency planning),
2. Lack of vulnerability/threat/risk assessment,
3. Lack of management involvement in computer security issues, and
4. Lack of protection against natural disasters.

Computer privacy problems include:

1. Manipulation of data (modification or falsification),
2. Acquisition of proprietary information without a "need-to-know," and
3. Unauthorized acquisition of passwords/algorithms.

What Can Be Done?

Security and privacy are two very important facets that a society, which is fast becoming automated, has to take into account. Although many things contribute to a lack or loss of security and privacy, the main ingredients in any security or privacy problem are the people involved with the systems. To most people, "security" and "privacy" are nebulous terms, and rather than learn all the rules and regulations concerning them, they choose to be apathetic. In order for society to have an effective and efficient computerized network, not only the systems themselves, but also all of the people involved with them, must be "geared" toward maintaining security and privacy. Security and privacy measures cannot be looked upon as unimportant or not pertinent, but must become an integral part of the computer environment.

This booklet was prepared by the Computer Sciences Department to promote awareness of computer security and privacy problems.

The Computer Sciences Department wishes to acknowledge the excellent response and assistance provided by Mr. J. Bonas, Graphics Branch, and Mr. W. J. Contorti, Technical Writing Branch, in planning this publication. Appreciation is also extended to Mr. D. W. Litton, Graphics Branch, for conceiving and preparing the artwork; to Ms. P. A. Ellis, Technical Writing Branch, for coordinating and writing the booklet; and to Mr. J. F. Neville, Jr., Programming and Computer Operations Branch, for his ideas and guidance.

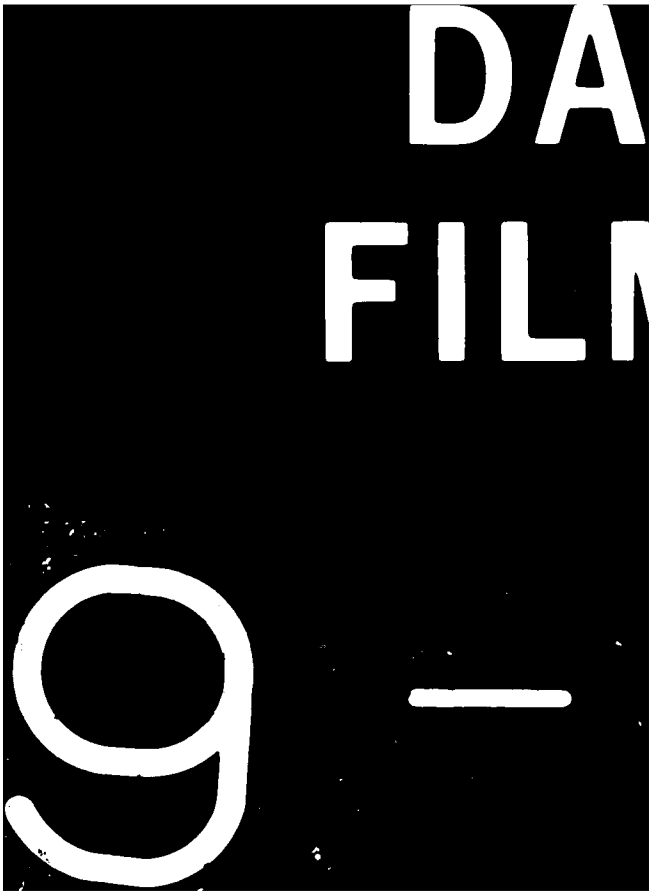
Questions and comments concerning the contents of this booklet should be directed to Mr. J. R. Babiec (Code 443).

Naval Underwater Systems Center
Technical Document 750

Approved for public release; distribution unlimited
1 August 1979

T. A. Galib

Head, Computer Sciences Department


DA
FILM
9 —